

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Chandar Kamalanathan, Fabiano DeSouza, Ching-Lung Tjiong, Reva Tolliver		
Assignee:	Dell Products L.P.		
Title:	System and Method for Secure HTML Links		
Serial No.:	10/777,600	Filed:	February 12, 2004
Examiner:	Teshome Hailu	Group Art Unit:	2439
Docket No.:	DC-06380	Customer No.:	33438

March 2, 2009

Filed Electronically

APPEAL BRIEF UNDER 37 CFR § 41.37

Dear Sir:

Applicants submit this Appeal Brief pursuant to the Notice of Appeal filed in this case on January 26, 2009. The fee for this Appeal Brief is being paid electronically via the USPTO EFS. The Board is authorized to deduct any other amounts required for this appeal brief and to credit any amounts overpaid to Deposit Account No. 502264.

I. REAL PARTY IN INTEREST - 37 CFR § 41.37(c)(1)(i)

The real party in interest is the assignee, Dell Products L.P., as named in the caption above and as evidenced by the assignment set forth at Reel 014987 Frame 0248.

II. RELATED APPEALS AND INTERFERENCES - 37 CFR § 41.37(c)(1)(ii)

Based on information and belief, there are no appeals or interferences that could directly affect or be directly affected by or have a bearing on the decision by the Board of Patent Appeals and Interferences in the pending appeal.

III. STATUS OF CLAIMS - 37 CFR § 41.37(c)(1)(iii)

Claims 1-20 are pending in the application. Claims 1-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over by U.S. Publication No. 2002/0069365 issued to Howard et al. in view of U.S. Patent Publication 2004/0250130 issued to Billharz et al. Appendix "A" contains the full set of pending claims.

IV. STATUS OF AMENDMENTS - 37 CFR § 41.37(c)(1)(iv)

No amendments after final have been requested or entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER - 37 CFR § 41.37(c)(1)(v)

Restricted browser functions that require a distinct user confirmation before execution of a selected function help protect users from malicious applications, but also are a nuisance where a browser interacts with a trusted server (page 2, line 18 - page 3, line 4). Claim 1 recites a system for secure HTML links (Figure 1, element 28; page 5, line 27) comprising a protocol encryption tool (Figure 1, element 12; page 5, line 10) that associates encrypted protocols with HTML links, an editor (Figure 1, element 16; page 5, line 19) that publishes an HTML link and associated encrypted protocol in a web page, a browser (Figure 1, element 26; page 5, line 26) that displays the web page and HTML link, the browser having one or more restricted functions that require at least selection of an HTML link and a function confirmation (Figure 1, element 36; page 6, line 2) before the browser executes the restricted function, and a protocol decryption engine (Figure 1, element 40; page 6, line 7) that decrypts the encrypted protocol to authorize execution of the restricted browser function without confirmation. Claim 9 recites a method for secure HTML links comprising encrypting a protocol associated with a restricted browser function (Figure 2, element 44; page 6, line 28), publishing the encrypted protocol in an HTML framework to associate with an HTML link that executes the restricted browser function (Figure 2, element 48, page 7, line 1), displaying the HTML framework through a browser that restricts execution of a restricted function by requiring a distinct confirmation (Figure 2, elements 50 and 52; page 7, line 2-4), decrypting the encrypted protocol at the browser (Figure 2, element 62; page 7, line 10) and authorizing execution of the restricted function without the distinct confirmation (Figure 2, element 64; page 7, line 11). Claim 18 recites an information handling system (Figure 1, element 10; page 5, line 10) comprising a browser (Figure 1, element 26; page 5, line 26) that retrieves and displays an HTML link associated with a restricted function, the browser requiring a distinct confirmation (Figure 1, element 36; page 5, line 32) of selection of the link before execution of the restricted function, an encrypted protocol (Figure 1, element 30; page 5, line 27) associated with the HTML link, and a protocol decryption engine (Figure 1, element 40; page 6, line 7) interfaced with the browser to override the distinct confirmation requirement upon decryption and validation of the encrypted protocol.

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL - 37 CFR § 41.37(c)(1)(vi)

Claims 1-20 stand improperly rejected under 35 U.S.C. § 103(a) as being unpatentable over by U.S. Publication No. 2002/0069365 issued to Howard et al. in view of U.S. Patent Publication 2004/0250130 issued to Billharz et al.

VII. ARGUMENT - 37 CFR § 41.37(c)(1)(vii)

Billharz and Howard cannot make obvious Claims 1, 10 or 17 because Billharz and Howard fail to teach, disclose or suggest all elements recited by Claims 1, 10 and 17. Accordingly, Applicants respectfully request that the Board reverse the rejections of the Examiner.

A. Claim 1

Claim 1 recites, in part, “a protocol decryption engine interfaced with the browser, the protocol decryption engine operable to decrypt the encrypted protocol associated with the HTML link and authorize execution of the associated restricted browser function without the function confirmation.”

Howard discloses a limited use browser that a client must run to download content in a view only mode.

Billharz discloses a “Yes/No” window which a user must select within one minute or the user will be signed out.

Howard and Billharz cannot make obvious Claim 1 because Howard and Billharz fail to teach, disclose or suggest all elements recited by Claim 1. For example, Howard and Billharz fail to teach, disclose or suggest “a protocol decryption engine interfaced with the browser, the protocol decryption engine operable to decrypt the encrypted protocol associated with the HTML link and authorize execution of the associated restricted browser function without the function confirmation” as recited by Claim 1. Howard does not disclose a protocol associated with an HTML link. Howard has a browser that decrypts content, the content restricted to read only, not a protocol associated with an HTML link. Howard teaches away from function confirmation before execution of a function because Howard downloads content, which has no function. The protocol recited by Applicants’ Claim 1 is associated with execution of a restricted browser function while the content presented by Howard performs no function. Billharz fails to disclose function confirmation as suggested by the Examiner. Billharz discloses a “Yes/No” window which a user must select within one minute or the user will be signed out from a secure link.

Billharz's "Yes/No" window does not confirm a request made by a client but rather appears when the client is inactive. Billharz teaches away from a combination with Howard: if the user of Howard requests a download of content, no need exists to confirm that the user is active; if the user of Billharz is inactive, no need exists to confirm a function; if the user of Billharz is active, and has made a request input, no need exists to establish that the client is active. Further, Billharz does not combine with Howard as suggested by the Examiner because no need would exist for a user of Howard to indicate activity since the user of Howard is attempting to download information. Accordingly, Applicant respectfully requests that the Board reverse the rejection of Claim 1.

B. Claim 9

Claim 9 recites, in part, "publishing the encrypted protocol in an HTML framework to associate with an HTML link that executes the restricted browser function;" "displaying the HTML framework through a browser, the browser restricting execution of restricted functions by requiring a distinct confirmation before execution of the restricted function" and "authorizing execution of the restricted function without the distinct confirmation."

In addition to the reasons set forth with respect to Claim 1, Claim 9 is allowable because neither Howard nor Billharz discloses "publishing the encrypted protocol in an HTML framework to associate with an HTML link that executes the restricted browser function." Presumably, the Examiner bases the rejections on the encryption of content by Howard which is downloaded and decrypted in a read only presentation. In contrast, Claim 9 recites "publishing the encrypted protocol ... to associate with an HTML link that executes the restricted browser function." Howard does not publish the encrypted protocol and is silent regarding the use of an HTML link that executes a restricted browser function or a need for a distinct confirmation. Accordingly, Applicants respectfully request that the Board reverse the Examiner's rejection of Claim 9.

C. Claim 18

Claim 17 recites, in part, "a protocol decryption engine interfaced with the browser and operable to override the distinct confirmation requirement upon decryption and validation of the encrypted protocol."

Neither Howard nor Billharz discloses a "distinct confirmation requirement" as recited by Claim 18. Billharz does not require "a distinct confirmation of a selection of the HTML link

before execution of the restricted function,” but rather presents a selection in response to inactivity by an end user. Nothing in Howard or Billharz discloses overriding a distinct confirmation requirement. Accordingly, Applicants respectfully request that the Board reverse the rejection of Claim 18.

VIII. CLAIMS APPENDIX - 37 CFR § 41.37(c)(1)(viii)

A copy of the pending claims involved in the appeal is attached as Appendix A.

IX. EVIDENCE APPENDIX - 37 CFR § 41.37(c)(1)(ix)

None.

X. RELATED PROCEEDINGS APPENDIX - 37 CFR § 41.37(c)(1)(x)

There are no related proceedings.

XI. CONCLUSION

For the reasons set forth above, Applicant respectfully submits that that rejection of pending Claims 1-20 is unfounded, and requests that the rejection of Claims 1-20 be reversed.

CERTIFICATE OF TRANSMISSION

I hereby certify that on March 2, 2009 this correspondence is being transmitted via the U.S. Patent & Trademark Office's electronic filing system.

/Robert W. Holland/

Respectfully submitted,

/Robert W. Holland/

Robert W. Holland
Attorney for Applicant(s)
Reg. No. 40,020

APPENDIX A

In the Claims

1. (Previously Presented) A system for secure Hypertext Markup Language (HTML) links, the system comprising:
 - a protocol encryption tool operable to associate encrypted protocols with HTML links, each protocol associated with a restricted browser function;
 - an editor operable to publish an HTML link and associated encrypted protocol in a web page;
 - a browser operable to display the web page and HTML link, the browser having one or more restricted functions, each restricted function requiring at least selection of an HTML link and a function confirmation before the browser executes the function; and
 - a protocol decryption engine interfaced with the browser, the protocol decryption engine operable to decrypt the encrypted protocol associated with the HTML link and authorize execution of the associated restricted browser function without the function confirmation.
2. (Original) The system of Claim 1 wherein the restricted browser function comprises a command to execute a binary.
3. (Original) The system of Claim 1 wherein the restricted browser function comprises a command to save a binary.
4. (Original) The system of Claim 1 wherein the restricted browser function comprises a command to execute a script.
5. (Original) The system of Claim 1 wherein the restricted browser function comprises a command to save a script.

6. (Original) The system of Claim 1 further comprising a protocol filter associated with the browser and operable to preprocess plural encrypted protocols upon retrieval of the web page by the browser.

7. (Original) The system of Claim 1 wherein the protocol encryption tool comprises a private key for encryption of protocols.

8. (Original) The system of Claim 7 wherein the protocol decryption engine comprises a public key.

9. (Original) A method for secure HTML links, the method comprising:
encrypting a protocol associated with a restricted browser function;
publishing the encrypted protocol in an HTML framework to associate with an HTML link that executes the restricted browser function;
displaying the HTML framework through a browser, the browser restricting execution of restricted functions by requiring a distinct confirmation before execution of the restricted function;
decrypting the encrypted protocol at the browser; and
authorizing execution of the restricted function without the distinct confirmation.

10. (Original) The method of Claim 9 wherein encrypting a protocol further comprises encrypting the protocol with a private key.

11. (Original) The method of Claim 10 wherein decrypting the protocol further comprises decrypting the protocol with a public key.

12. (Original) The method of Claim 11 wherein authorizing execution of the restricted function further comprises authorizing execution of a binary by the browser.

13. (Original) The method of Claim 11 wherein authorizing execution of the restricted function further comprises authorizing saving of a binary by the browser.

14. (Original) The method of Claim 11 wherein authorizing execution of the restricted function further comprises authorizing execution of a script by the browser.

15. (Original) The method of Claim 11 wherein authorizing execution of the restricted function further comprises authorizing saving of a script by the browser.

16. (Original) The method of Claim 11 further comprising preprocessing of plural encrypted protocols substantially upon loading of the HTML framework to the browser.

17. (Original) The method of Claim 11 wherein the distinct confirmation comprises a window displayed upon user selection of an HTML link associated with a restricted function, the window requiring at least one addition input by the user before execution of the restricted function.

18. (Original) An information handling system comprising:
a browser operable to retrieve and display a HTML link associated with a restricted function, the browser requiring a distinct confirmation of a selection of the HTML link before execution of the restricted function;
an encrypted protocol associated with the HTML link;
a protocol decryption engine interfaced with the browser and operable to override the distinct confirmation requirement upon decryption and validation of the encrypted protocol.

19. (Original) The information handling system of Claim 18 wherein the browser is further operable to retrieve a web page having plural encrypted protocols, the information handling system further comprising a protocol filter interfaced with the browser and operable to identify the plural encrypted protocols for decrypting by the protocol decryption engine.

20. (Original) The information handling system of Claim 19 further comprising a protocol database interfaced with the protocol decryption engine and having a table of protocols and associated restricted functions.

EVIDENCE APPENDIX - 37 CFR § 41.37(c)(1)(ix)

None.

RELATED PROCEEDINGS APPENDIX - 37 CFR § 41.37(c)(1)(x)

There are no related proceedings.